Informe de Análisis de Cabeceras HTTP

Fecha del Análisis

1 de octubre de 2024

Sitios Analizados

A continuación se presentan los sitios web que han sido analizados junto con sus respectivas cabeceras HTTP y el análisis correspondiente.

1. Sitio Web: rosenbergcanada.com

Cabeceras HTTP

Análisis

- **Strict-Transport-Security**: No presente. Se recomienda habilitar HSTS para mejorar la seguridad.
- **Content-Security-Policy**: No presente. Se recomienda establecer políticas para mitigar ataques de inyección de contenido.
- **X-Frame-Options**: No presente. Considerar agregarlo para prevenir ataques de clickjacking.
- **X-Content-Type-Options**: No presente. Se sugiere incluirlo para prevenir el tipo de contenido MIME.
- **Server Banner**: Visible (Apache). Se recomienda ocultar esta información.

2. Sitio Web: ecfangrid.ca

Cabeceras HTTP

Análisis

- **Strict-Transport-Security**: No presente. Se recomienda habilitar HSTS para mayor seguridad.
- **Content-Security-Policy**: No presente. Recomendable para mitigar ataques de inyección de contenido.

- **X-Frame-Options**: No presente. Considerar su inclusión para prevenir clickjacking.
- **X-Content-Type-Options**: No presente. Añadir para prevenir el tipo de contenido MIME.
- **Server Banner**: Visible (Apache). Se sugiere ocultar esta información.

3. Sitio Web: m.ecfangrid.ca

Cabeceras HTTP

Análisis

- **Conexión Segura**: Hubo un error al intentar verificar la legitimidad del servidor, lo que impidió establecer una conexión segura. Se recomienda revisar el certificado SSL del servidor y asegurarse de que sea válido.
- **Strict-Transport-Security**: No presente. Se recomienda habilitar HSTS para mayor seguridad.
- **Content-Security-Policy**: No presente. Recomendable para mitigar ataques de inyección de contenido.
- **X-Frame-Options**: No presente. Considerar su inclusión para prevenir clickjacking.
- **X-Content-Type-Options**: No presente. Añadir para prevenir el tipo de contenido MIME.
- **Server Banner**: Visible (Apache). Se sugiere ocultar esta información.

Conclusiones Generales

Los análisis de las cabeceras HTTP para los sitios web mencionados indican que, aunque hay algunas medidas de seguridad en su lugar, hay áreas significativas que requieren atención. La ausencia de cabeceras de seguridad críticas como HSTS, Content Security Policy y otras, sugiere que se pueden realizar mejoras para proteger mejor estos sitios contra vulnerabilidades comunes.

Acciones Recomendadas

1. **Habilitar HSTS**: Esto obligará a los navegadores a usar HTTPS, mejorando la seguridad general del sitio.
2. **Implementar Content Security Policy**: Esto ayudará a prevenir ataques como el cross-site scripting (XSS).
3. **Agregar X-Frame-Options**: Para proteger contra ataques de clickjacking.

4. **Incluir X-Content-Type-Options**: Para prevenir que el navegador interprete archivos de un tipo diferente al indicado.
5. **Ocultar la información del servidor**: Para reducir el riesgo de ataques dirigidos basados en información del servidor.
6. **Mantener el software actualizado**: Asegurarse de que todas las versiones de software estén actualizadas para reducir vulnerabilidades.
7. **Revisar el Certificado SSL**: Asegurarse de que sea válido y esté correctamente configurado para establecer conexiones seguras.

Firmado

Este informe ha sido preparado como parte de una auditoría de seguridad para evaluar la configuración de los sitios analizados.